# Secure Access migration checklist

**To make your network safer and more secure from cyber attacks, we need to make some crucial changes to the way all users and devices at your school or kura access your Wi-Fi. The purpose of Secure Access migration day is to enrol as many devices at your school as possible to your new Secure Access network.**

We'll be assigning one of our trusted IT partners to your school to work with your nominated Secure Access contacts to get everything prepared for the day.

As well as enrolling all your devices on migration day, your assigned IT partner will train your nominated Secure Access contacts, including your IT provider (if you have one) on how to enrol new staff and student devices on to your new network in the future.

## What do we classify as a device?

Devices are any laptops, desktops, phones, Chromebooks, iPads used by your school or kura that are funded by the Ministry of Education. This funding covers their migration to the new Secure Access Wi-Fi network.

*While our team is working with your school we'll try to enrol as many additional BYOD devices as possible that are brought to school on migration day. However, Ministry-funded devices have the priority so we can't guarantee all BYOD devices will be enrolled.*

## What do we mean by a third-party device?

Third-party devices are any pieces of infrastructure that connect to your network. The cost of migrating these falls to your school as they may require vendor-specific support.

These devices can include those connected on your school's Internet of Things (IoT) such as VoIP phones, solar panels and their controllers, heat pumps, building management and security systems e.g. IP cameras, digital screens, CCTV, PA systems, fire alarm systems, building access e.g. swipe card, Wi-Fi calling, and other customised equipment that requires to be connected to your school's network.

You may have multiple third-party device providers: for example the suppliers of your fire alarm system may differ from your heat pump installers.

*If you are considering upgrading your equipment, we suggest doing so before migration day as their performance might be impacted by the migration, for example if they have an outdated operating system.*

| Time | Task | ☑ |
|---|---|---|
| Pre-migration day | **Enrol all school-owned Chromebooks in Google Workspace and/or get a Mobile Device Management system**<br><br>It will make the migration and managing the devices in the future easier. | ☐ |
| | **Identify any end-of-life devices**<br><br>As any end-of-life devices that are not supported by their manufacturer, can't be managed by your school's Mobile Device Management system (if one is in place) and will have to be enrolled manually to the new Secure Access network. You can check the list of unsupported devices on the manufacturer websites:<br><br>• Chromebooks<br>• iPhones<br>• iPads. | ☐ |
| | **Arrange to enrol your third-party devices**<br><br>A guideline to what counts as a third-party device is provided above. Your IT support or IT provider (or the device provider) may be able to assist with this step. | ☐ |
| | **Schedule 2 Secure Access visits**<br><br>Once we've assigned an IT partner to your school, we'll arrange the dates for your Technical Survey and migration day. You'll need to agree on suitable times and locations for the various steps of the Migration Plan, including a dedicated time and space for BYOD enrolments where students and staff can gather with their devices.<br><br>*Migration takes 1 day for most schools, although it can take longer for larger schools, and should be scheduled on a day when most staff and students are available.* | ☐ |
| | **Finalise your Migration Plan**<br><br>Your assigned IT partner will visit your school and work with your nominated Secure Access contact to agree the migration scope (Technical Survey) and finalise the Migration Plan. This includes key decisions relating to your guest access type your school has chosen, as well as your filtering and firewall policies, and there may be changes to the current state of these that you need to be aware of.<br><br>*The IT partner needs to be granted access to your school's user directory to allow integration with the Secure Access systems - note N4L will have read-only access to your user directory to support lifecycle management of your users.* | ☐ |
| | **Acknowledge Technical Survey**<br><br>Confirm that you've been briefed by your assigned IT partner of the migration day details and the Technical Survey has been filled out. | ☐ |

## Week before migration day

**Plan for all devices to be enrolled to be available on the migration day** ☐

Including any BYOD devices students or staff may have at home.

**Check over your third-party device inventory** ☐

Contact any differing providers who may be needed to advise on migrating your third-party devices to Secure Access: e.g. fire alarm systems.

**Locate power points and make sure they are accessible** ☐

It's likely you'll need more power points than a standard school day.

**Check batteries on remote controls for TVs and monitors** ☐

If your school uses Apple TVs or similar tech you'll need these to access settings.

**Have the location of your casting devices ready** ☐

Your casting devices will be enrolled to the Staff network. This will provide kaiako with the ability to share content from student devices via casting through existing school collaboration tools, e.g. Google Meet, Microsoft Teams or Zoom.

**Ensure all appropriate school staff have access to MyN4L** ☐

They will need to use the Device Registration and Guest Access tools in MyN4L to manage devices and guest use of your school network.

## Migration day

**Ensure your assigned IT partner has full access to the school buildings** ☐

As per the agreed Migration Plan.

**Make sure all devices are onsite, fully charged, with passwords handy** ☐

Having a schedule to enrol devices used in classes will mean less disruption to learning.

**Your IT contact needs to be present** ☐

Your nominated Secure Access contact will need to be available at least for testing at the start and end of the day, as well as acceptance sign-off at the very end of migration day. Having your IT support or IT provider available during the migration day will also be useful when it comes to the enrolment of various devices.

**Assemble your team to be trained** ☐

Your team needs to receive training on how to enrol devices to new Wi-Fi networks. This includes anyone who might be involved in welcoming visitors to the school and sharing guest access, and shouldn't take longer than 1 hour.

*It's important your staff are trained before your assigned IT partner leaves.*

**Check your printer settings on individual user devices after printer migration** ☐

Printer settings may require reconnecting after printers have migrated.

**Sign off your test plans** ☐

When migration is completed, we'll need your assigned Secure Access contact to sign off our test plans via Support Hub.

## Post-migration day support

### Ongoing support

Following the migration you can contact our friendly Customer Support team on **0800 LEARNING** if you experience any issues with your devices or network.

We welcome all feedback. If required, we'll contact your assigned IT partner within their 30-day warranty support period to arrange remediation.

We'll stay in touch throughout the process and remind you of the steps above to make your migration as smooth as possible. For more information see the post-migration support guidance or Support Hub.

### Get in touch

You can reach out to our Customer Support team on **0800 LEARNING** Monday – Friday, 8am to 5pm, while your School Relationship Manager is also on hand to support you.